

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently amended) A method of protecting a data center against a
2 denial of service attack, the method comprising: sending queries to data
3 collectors, deployed at different points in a network that carries network traffic to
4 the data center, the data collectors collect statistical information on network
5 packets sent over the network, the queries to request the statistical information
6 from at least some of the data collectors; ~~and~~
7 sending the statistical information from the data collectors in response to
8 the queries; and
9 processing the statistical information to determine the source of suspicious
10 network traffic sent to the data center by aggregating statistical information of
11 traffic flows from a source address and source port to a destination address and
12 destination port, measured over different periods of time.

1 2. (Currently amended) The method of claim 1 wherein the network
2 packets from the attacker have faked, random source addresses that change with
3 time, and sending queries further comprises:
4 sending queries to the data collectors for the statistical information based
5 on ~~victim~~ destination address for the data center.

1 3. (Currently amended) The method of claim 1 wherein processing further
2 comprises:

3 determining, from at least in part, the collected statistical information,
4 what data centers are involved in the attack on the ~~victim~~-data center.

1 4. (Currently amended) The method of claim 3 wherein determining is
2 performed by a control center that receives the statistical information from the
3 data collectors, and determining further comprises:
4 sending data to/from a gateway device that is associated with the ~~victim~~
5 data center.

1 5. (Currently amended) The method of claim 4 wherein the gateway
2 identifies the network address of the data center-~~victim~~, via a message to the
3 control center.

1 6. (Previously Presented) The method of claim 1 wherein the queries and
2 the statistical information are sent over a redundant network that does not carry
3 the packet traffic to deliver collected statistical information to a central control
4 center in response to the queries sent from the central control center.

1 7. (Original) The method of claim 5 wherein message indicates the type of
2 attack.

1 8. (Previously Presented) The method of claim 1 wherein a source of the
2 attack is behind a gateway.

1 9. (Previously Presented) The method of claim 8 wherein if a source of the
2 attack is behind a gateway, the control center issues a request to the gateway that
3 the attacking system is behind to prevent the attacking traffic from attacking
4 system from reaching the network.

1 10. (Currently amended) The method of claim 8 wherein if a source of the
2 attack is behind a gateway, the gateway that the attacking system is behind
3 selectively discards traffic that appears to be malicious traffic and that contains
4 the ~~victim~~-destination address of the data center.

1 11. (Previously presented) The method of claim 1 wherein if a source of
2 the attack is not behind a gateway, a control center queries the data collectors to
3 provide information about possible locations of the attacking system.

1 12. (Previously presented) The method of claim 1 wherein if a source of
2 the attack is not behind a gateway, the method further comprises:
3 contacting administrators at locations involved in the attack to have the
4 administrators take action to filter out packets with a destination address.

1 13. (Currently amended) The method of claim 1 wherein the attack is a
2 low-grade spoofing-type of attack that does not compromise network traffic flow
3 between the ~~victim~~-data center and Internet.

1 14. (Currently amended) The method of claim 1 wherein the attack is a
2 high-grade attack that compromises network traffic flow between the ~~victim~~-data
3 center and Internet.

1 15. (Previously presented) A method of protecting a victim data center
2 against a denial of service attack, the method comprising:
3 receiving packets with faked, random source addresses;
4 receiving, from a gateway disposed near the victim data center, a
5 notification that the victim data center is under an attack; sending queries to data
6 collectors deployed at different points in a network that carries network traffic to

7 the victim data center, the data collectors to sample network packets and collect
8 statistical information on network packets sent over the network, the queries
9 being requests for statistical information from data collectors that have examined
10 network traffic with a victim destination address; and
11 determining a data center or centers involved in the attack on the victim
12 data center by analyzing collected statistical information from the data collectors,
13 wherein the analyzing comprises aggregating statistical information of traffic
14 flows from a source address and source port to a destination address and
15 destination port, measured over different periods of time.

1 16. (Currently amended) The method of claim 15 further comprising:
2 communicating statistical information from a control center to/from a
3 gateway device that is disposed with the ~~victim~~-data center.

1 17. (Previously Presented) The method of claim 16 wherein if a source of
2 the attack is behind a gateway, the control center issues a request to the gateway
3 to block the attacking traffic.

1 18. (Previously Presented) The method of claim 17 wherein if a source of
2 the attack is behind a gateway, the gateway selectively discards traffic that
3 appears to be malicious traffic and that contains the victim destination address.

1 19. (Previously presented) The method of claim 15 wherein if a source of
2 the attack is not behind a gateway, the method comprises:
3 contacting administrators at locations involved in attack to filter out
4 packets having a destination address.

1 20. (Currently amended) A system to thwart denial of service attacks on a
2 victim data center, the system comprising: a plurality of data collectors monitors
3 dispersed throughout a network, the data collectors monitors collecting statistical
4 data on network traffic;
5 a control center coupled to the plurality of data collectors, the control
6 center, comprising
7 a memory;
8 a processor; and
9 ~~executing~~ a computer readable medium storing a computer program
10 product, the ~~stored on a~~ computer readable medium[[,]] comprising instructions
11 for causing the control center ~~a computer~~ to:
12 receive from the data center ~~victim site~~ a notification that the victim data
13 center is under an attack; and in response to receiving the notification,
14 send queries to data collectors to request ~~the~~ statistical information ~~from~~
15 collected by the data collectors based on network traffic, the statistical
16 information used to determine a source of suspicious network traffic being sent to
17 the data center ~~victim~~, wherein determining ~~the~~ a source of suspicious network
18 traffic comprises aggregating statistical information of traffic flows from a source
19 address and source port to a destination address and destination port, measured
20 over different periods of time;
21 a gateway device that passes network packets between the network and
22 the ~~victim~~ data center, the gateway disposed to protect the victim data center, and
23 being coupled to the control center.

1 21. (Previously Presented) The system of claim 20 wherein the data
2 collectors collect statistical information on network packets that pass through
3 points in the network that the data collectors monitor.

1 22. (Currently amended) The system of claim 20 wherein the control
2 center further comprises instructions to:
3 determine a source of the attack on the ~~victim~~-data center by analyzing
4 collected statistical information from the data collectors.

1 23. (Currently amended) The system of claim 20 wherein the control
2 center and gateway device associated with the ~~victim~~-data center exchange data
3 including statistical information to thwart the attack.

1 24. (Previously presented) The system of claim 20 wherein data
2 exchanged between the control center and gateway device associated with the
3 victim data center are sent over a redundant network that is a different network
4 than the network that is being monitored by the data collectors.

1 25. (Previously Presented) The system of claim 20 wherein if the control
2 center determines that the source of the attack is behind a gateway, the control
3 center issues a request to the gateway that the source of the attack is behind to
4 block the attacking traffic.

1 26. (Currently amended) The system of claim 20 wherein if the control
2 center determines that the source of the attack is behind a gateway, the control
3 center issues a request to the gateway to selectively discard traffic that contains a
4 ~~the victim~~-destination address for the data center.

1 27. (Previously Presented) The system of claim 20 wherein if the source of
2 the attack is not behind a gateway, the control center queries the data collectors to
3 provide information about possible locations of the source of the attack.

1 28. (Currently amended) The system of claim 27 wherein if the source of
2 the attack is not behind a gateway, the system includes instructions to contact
3 administrators at locations involved in attack to have the administrators cause
4 filters to be installed in the data center ~~take action~~ to filter out packets with the
5 victim destination address.

1 29. (Currently amended) A computer program product residing on a
2 computer readable media for protecting a victim data center against a denial of
3 service attack, the computer program product, comprising instructions for causing
4 a computing device to:
5 receive a notification that the victim data center is under an attack;~~send~~
6 send queries to data collectors deployed at different points in a network that
7 carries network traffic to the victim data center, the data collectors to sample
8 network traffic and collect statistical information on packets sent over the
9 network, the queries to request statistical information from data collectors that
10 have examined network traffic with the victim destination address; and
11 determine a source of the attack on the victim data center by analyzing
12 collected information from the data collectors, wherein the analyzing comprises
13 aggregating statistical information of traffic flows from a source address and
14 source port to a destination address and destination port, measured over different
15 periods of time.

1 30. (Previously Presented) The computer program product of claim 29
2 further comprising instructions to:
3 send data including statistical information between a gateway device that
4 is disposed with the victim data center and a control center.

1 31. (Previously Presented) The computer program product of claim 29
2 further comprising instructions to:
3 determine whether the source of the attack is behind a gateway and if the
4 source of the attack is behind a gateway,
5 issue a request to the gateway to block the attacking traffic.

1 32. (Previously Presented) The computer program product of claim 29
2 further comprising instructions to:
3 determine whether the source of the attack is behind a gateway and if the
4 source of the attack is not behind a gateway,
5 send a message to contact administrators at locations involved in the
6 attack to filter out packets having the destination address.

1 33. (Previously Presented) The method of claim 1 further comprising:
2 receiving from the victim site a notification that the victim site is under an
3 attack.